

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-76139  
(P2000-76139A)

(43) 公開日 平成12年3月14日 (2000.3.14)

|                           |       |               |                   |
|---------------------------|-------|---------------|-------------------|
| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I           | テマコード (参考)        |
| G 0 6 F 12/14             | 3 2 0 | G 0 6 F 12/14 | 3 2 0 D 5 B 0 1 7 |
| G 0 6 K 19/073            |       | G 0 6 K 19/00 | P 5 B 0 3 5       |

審査請求 未請求 請求項の数 2 O L (全 5 頁)

(21) 出願番号 特願平10-243380

(22) 出願日 平成10年8月28日 (1998.8.28)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 丹野 雅明

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 竹田 忠雄

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74) 代理人 100064621

弁理士 山川 政樹

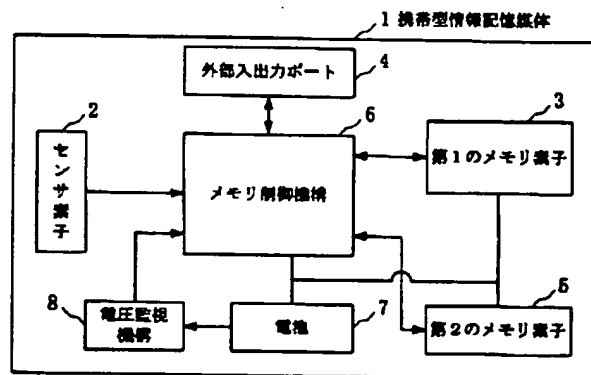
最終頁に続く

(54) 【発明の名称】 携帯型情報記憶媒体

(57) 【要約】

【課題】 外部からの物理的な攻撃を検知したとき、機密情報を消去すると共に必要な情報を保存する。

【解決手段】 センサ素子2は外部からの物理的な攻撃を検知する。第1のメモリ素子3は書き込み読み出し可能なメモリで、第2のメモリ素子5は一度だけ書き込み可能な読み出し専用のメモリである。電圧監視手段8は電池7の出力電圧を監視する。メモリ制御機構6は、センサ素子2によって物理的な攻撃が検知されたとき、あるいは電圧監視機構8によって電池7の出力電圧異常が検知されたとき、メモリ素子3から保存すべき情報を読み出してメモリ素子5に書き込むと共に、メモリ素子3に記憶された機密情報を消去する。



## 【特許請求の範囲】

【請求項1】 外部からの物理的な攻撃を検知するセンサ素子と、

書き込み読み出し可能な第1のメモリ素子と、

一度だけ書き込み可能な読み出し専用の第2のメモリ素子と、

センサ素子の応答に連動するメモリ制御手段とを有し、前記メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第1のメモリ素子から保存すべき情報を読み出して第2のメモリ素子に書き込むと共に、第1のメモリ素子に記憶された機密情報を消去することを特徴とする携帯型情報記憶媒体。

【請求項2】 請求項1記載の携帯型情報記憶媒体において、

電力供給用の電池と、

この電池の出力電圧を監視する電圧監視手段とを有し、前記メモリ制御手段は、電圧監視手段によって電池の出力電圧異常が検知されたとき、第1のメモリ素子から保存すべき情報を読み出して第2のメモリ素子に書き込むと共に、第1のメモリ素子に記憶された機密情報を消去することを特徴とする携帯型情報記憶媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ICカードに代表される携帯可能な小型情報記憶媒体のセキュリティに関し、詳しくはICカード等の記憶情報を不正に解析することを阻害すると共に、重要な記憶情報を不正な攻撃から防御する技術に関するものである。

## 【0002】

【従来の技術】従来より、機密情報等を記憶する情報記憶媒体として、不正な物理的攻撃から記憶情報を守るために、物理的なセキュリティ機構を内蔵するものが提案されている。代表的な例として、米国IBM社の $\mu$ ABYSS（参考文献：S.H.Weigart, "Physical security for the  $\mu$ ABYSS system", Proc. 1987 IEEE Symp. on Security and Privacy, Oakland, CA, pp. 52-58, April 1987）がある。

【0003】この $\mu$ ABYSSは、モジュール全体が金属細線で筒状に包まれており、金属細線を切断しない限り、モジュール内部を観測することができない。金属細線が切断された場合、モジュールに内蔵されたセキュリティ機構が金属細線の抵抗変化を検知し、即座に機密情報を消去する。これによって機密情報の漏洩を防止するものである。このほかのセキュリティ機構を内蔵する情報記憶媒体も外部からの攻撃を感知すると重要な情報を消去する動作を行っている。

## 【0004】

【発明が解決しようとする課題】以上のように、従来の情報記憶媒体のセキュリティ機構は、機密情報を消去することによってその漏洩を防止するため、セキュリティ

機構が攻撃を検知した後は、情報記憶媒体に対し正規の情報読み出し操作を行っても、当然の事ながら機密情報を読み出すことは不可能となる。このようなセキュリティ機構を内蔵した携帯型情報記憶媒体をプリペイドカードや電子マネーカードに適用した場合、故意、過失あるいは事故によってセキュリティ機構が動作すると、カード内の残額データが消去されるため、カードの貨幣価値を復元できないという問題点があった。また、内蔵電池が消耗し、必須のデータが失われるという問題点もあった。このような問題は、電池切れや事故等により破損したプリペイドカードを、窓口で交換する際、新しいプリペイドカードに投入する残高データの根拠がないことになり、カード運用会社と利用者の何れかが金銭的被害を被ることとなる。本発明は、上記課題を解決するためになされたもので、外部からの物理的な攻撃を検知したとき、機密情報を消去すると共に必要な情報を保存することができる携帯型情報記憶媒体を提供することを目的とする。また、内蔵電池に対する攻撃や電池の消耗を検知したとき、機密情報を消去すると共に必要な情報を保存することができる携帯型情報記憶媒体を提供することを目的とする。

## 【0005】

【課題を解決するための手段】本発明の携帯型情報記憶媒体は、請求項1に記載のように、外部からの物理的な攻撃を検知するセンサ素子（2）と、書き込み読み出し可能な第1のメモリ素子（3）と、一度だけ書き込み可能な読み出し専用の第2のメモリ素子（5）と、センサ素子の応答に連動するメモリ制御手段（6）とを有し、上記メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第1のメモリ素子から保存すべき情報を読み出して第2のメモリ素子に書き込むと共に、第1のメモリ素子に記憶された機密情報を消去するものである。このように、メモリ制御手段は、センサ素子によって物理的な攻撃が検知されたとき、第1のメモリ素子から保存すべき情報を読み出して第2のメモリ素子に書き込むと共に、第1のメモリ素子に記憶された機密情報を消去するので、機密漏洩の防止と必要な情報の保存を両立させることができる。また、請求項2に記載のように、電力供給用の電池（7）と、この電池の出力電圧を監視する電圧監視手段（8）とを有し、上記メモリ制御手段は、電圧監視手段によって電池の出力電圧異常が検知されたとき、第1のメモリ素子から保存すべき情報を読み出して第2のメモリ素子に書き込むと共に、第1のメモリ素子に記憶された機密情報を消去するので、機密漏洩の防止と必要な情報の保存を両立させる

ことができる。

#### 【0006】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。図1は本発明の実施の形態となる携帯型情報記憶媒体の構成を示すブロック図である。本実施の形態の携帯型情報記憶媒体1は、外部からの物理的な攻撃を検知するセンサ素子2と、書き込み読み出し可能な第1のメモリ素子3と、外部のリーダー/ライタ等とデータのやり取りをするための外部入出力ポート4と、一度だけ書き込み可能な読み出し専用の第2のメモリ素子5と、センサ素子2によって物理的な攻撃が検知されたとき、あるいは後述する電圧監視機構によって電池の出力電圧異常が検知されたとき、第1のメモリ素子3から保存すべき情報を読み出して第2のメモリ素子5に書き込むと共に、第1のメモリ素子3に記憶された機密情報を消去するメモリ制御機構6と、第1、第2のメモリ素子3、5、メモリ制御機構6等に電力を供給するための電池7と、電池7の出力電圧を監視する電圧監視機構8とを有している。

【0007】センサ素子2は、外部からの物理的な攻撃（封止材の開封などの不正な行為と見なされる物理的な刺激）を検知するセンサであり、媒体1の封止材が開封されたことによる内部への入射光を検知する受光素子、封止部分の電気抵抗若しくは静電容量の所定量以上の変化を検知する電子回路、あるいは所定量以上の衝撃を検知する衝撃センサ等によって構成される。封止部分の電気抵抗の変化を検知する電子回路は、封止材内に図1の構成を光学的に遮蔽するように設けられた金属板の電気抵抗を測定するものであり、外部からの攻撃によって金属板が取り外されたことによる電気抵抗の変化を検知するものである。封止部分の静電容量の変化を検知する電子回路は、封止材を挟んで対向する上記金属板との間の静電容量を測定するものであり、外部からの攻撃によって金属板が取り外されたことによる静電容量の変化を検知するものである。

【0008】第1のメモリ素子3は、暗号キーや個人認証情報、残金や積立ポイント数等の機密情報を記憶すると共に、一時記憶用のワークメモリとして使用されるメモリであり、RAM (Random Access Memory) 等の揮発性メモリあるいはEEPROM (Electrically Erasable and Programmable Read Only Memory) 等の不揮発性メモリによって構成される。

【0009】第2のメモリ素子5は、一度だけ電氣的に書き込み可能な不揮発性メモリであり、ワンタイムPROM (Programmable Read Only Memory) によって構成される。このワンタイムPROMには、メモリセル毎にヒューズを設け、データ書き込みの際にヒューズを溶断するヒューズ溶断型等がある。なお、第2のメモリ素子5は、未書込状態のまま媒体1に搭載される。

【0010】メモリ制御機構6としては、例えばコンピ

ュータのメモリマネージメントユニット (MMU) やマイクロプロセッサ等の中央処理装置 (CPU) を用いてもよい。次に、本実施の形態の携帯型情報記憶媒体1が外部からの攻撃を受けた場合の動作を説明する。図2は媒体1が攻撃を受けた際の動作を示すフローチャート図である。

【0011】センサ素子2によって物理的な攻撃が検知されたとき、あるいは電圧監視機構8によって電池7の出力電圧異常が検知されたとき（図2ステップ101）、メモリ制御機構6は、第1のメモリ素子3内にある機密情報の記憶領域から残金や積立ポイント数等の保存すべき情報を読み出し、読み出した情報を第2のメモリ素子5に書き込む（ステップ102）。続いて、メモリ制御機構6は、第1のメモリ素子3内にある機密情報の記憶領域に対して、書き換えを行うことにより、機密情報を消去する（ステップ103）。

【0012】以上のように、本実施の形態の携帯型情報記憶媒体1では、物理的な攻撃が検知されたとき、あるいは電池7の取り外し若しくは消耗による電池7の出力電圧異常が検知されたとき、機密情報を消去するので、機密情報の解読を不可能にすることができる。また、機密情報のうち、保存が必要な情報に関しては、メモリ制御機構6が第2のメモリ素子5に書き込む。

【0013】例えば、プリペイドカードや電子マネーカードあるいはポイントカードに本発明の携帯型情報記憶媒体を適用する場合、暗号キーや個人認証情報等の機密情報をカード内のメモリ素子3から抹消し、残高データや積立ポイント数についてはメモリ素子5に書き込んだ上で、元々の記憶領域から抹消する。これにより、カードに対して故意に攻撃が加えられた場合には、セキュリティ機構が動作して機密情報の漏洩を防ぐことができ、偶発的な事故によってセキュリティ機構が動作した場合でも、残金等の情報を保存することが可能となる。

【0014】したがって、残金等のプリペイドカードを故意に破壊すると、このカードの第2のメモリ素子5に残金が零であることが記録され、しかも一度だけ書き込みが可能なメモリ素子5の情報を書き換えることはできないので、残金等のカードを故意に破壊した者が、カードが不良になったと申告して不法に換金することを防ぐことができる。また、カードを開封すると、第2のメモリ素子5への書き込みが行われるので、第2のメモリ素子5の書込状態を確認すれば、カードに対して攻撃が加えられたか否かを確認することができる。よって、カードを不正に開封した後に、カードを封止して正常なカードを装ったとしても、被害を受けたカードであるか否かを判断することが可能となる。

【0015】なお、電池7には図示しないコンデンサが並列に配設されており、このコンデンサに蓄えられた電荷により、電池7が取り外された場合でも、図2の動作を行えるようになっている。また、本発明の携帯型情報

記憶媒体1は、樹脂製のカードに半導体チップを埋め込んだICカードの形態であってもよいし、薄型部品を薄型ケースに組み込んだPCMCIA(PCカード)の形態であってもよい。また、センサ素子2、メモリ素子3、5、メモリ制御機構6、電圧監視機構8を独立した部品で構成してもよいし、1チップに集積した構成でもよい。

#### 【0016】

【発明の効果】本発明によれば、請求項1、2に記載のように、センサ素子、第1のメモリ素子、第2のメモリ素子及びメモリ制御手段を設けることにより、外部からの不正な攻撃や偶発的な事故や内蔵電池の消耗等に連動して、機密情報の消去と保存すべき情報の保持を行うため、機密漏洩の防止と必要な情報の保存を両立させることができる。動作解析や記憶情報の解読のために、本携帯型情報記憶媒体を不正に開封すると、即座に機密情報が消去されるため、暗号化手順、暗号キー、記憶領域のフォーマット等、解読に重要な情報を漏洩から守ることができる。仮に、第2のメモリ素子に書き込んだ情報が解読されたとしても、第1のメモリ素子に書き込まれていた機密情報が消去されているので、本来の機密情報を復元することは不可能となる。本携帯型情報記憶媒体を

プリペイドカードやポイントカードに適用した場合、偶発的な事故や内蔵電池の消耗により使用できなくなった携帯型情報記憶媒体をサービスの運営機関に持参すれば、新しい携帯型情報記憶媒体に必要な情報をコピーすることができる。また、残金等の携帯型情報記憶媒体を故意に破壊した者が、媒体が不良になったと申告して不法な換金を要求する犯罪にも対処でき、携帯型情報記憶媒体を不正に開封した後に封止し直して正常な媒体を装ったとしても、第2のメモリ素子の書込状態を確認することで、被害を受けた媒体であるか否かを判断することができる。

#### 【図面の簡単な説明】

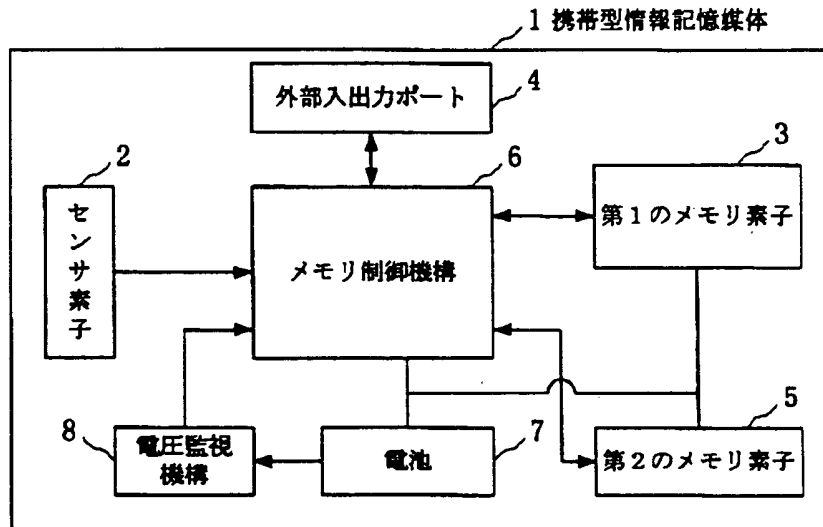
【図1】 本発明の実施の形態となる携帯型情報記憶媒体の構成を示すブロック図である。

【図2】 図1の携帯型情報記憶媒体が攻撃を受けた際の動作を示すフローチャート図である。

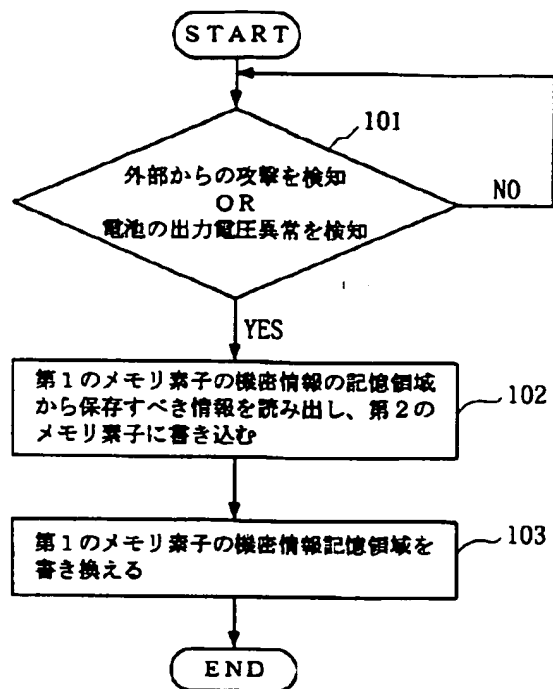
#### 【符号の説明】

1…携帯型情報記憶媒体、2…センサ素子、3…第1のメモリ素子、4…外部入出力ポート、5…第2のメモリ素子、6…メモリ制御機構、7…電池、8…電圧監視機構。

【図1】



【図2】



フロントページの続き

(72)発明者 伴 弘司

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

Fターム(参考) 5B017 AA03 AA08 BA08 CA14  
5B035 AA15 BB09 CA38

**THIS PAGE BLANK (USPTO)**